INFORMATION SECURITY MANAGER

Purpose:

To actively support and uphold the City's stated mission and values. To establish and maintain the enterprise vision, strategy and program to ensure information assets and technologies are adequately protected. To develop strategic policy, technology plans and infrastructure investment recommendations that mitigate overall risks, strengthen data defenses and reduce vulnerabilities for internal and public facing systems.

Supervision Received and Exercised:

Receives direction from the Deputy Internal Services Director – Information Technology

Exercises direct supervision of personnel in related area of responsibility;

Exercises technical and functional direction over vendors and contract staff.

Essential Functions:

Duties may include, but are not limited to, the following:

- Develop, implement and monitor a strategic, comprehensive enterprise information security program to ensure that the integrity, confidentiality and availability of information is owned, controlled or processed by the organization.

- Facilitate information security governance through the implementation of a governance program, including an information security steering committee or advisory board.

- Develop, maintain and publish up-to-date information security policies, standards and guidelines. Oversee the approval, training, and dissemination of security policies and practices.

- Create, communicate and implement a risk-based process for vendor risk management, including the assessment and treatment for risks that may result from partners, consultants and other service providers.

- Develop and manage information security budgets, and monitor them for variances.

- Create and manage information security and risk management awareness training programs for all employees, contractors and approved system users.

- Create a framework for roles and responsibilities with regard to information ownership, classification, accountability and protection.

- Develop and enhance an information security management framework based on ISO2700X,

- Provide strategic risk guidance for IT projects, including the evaluation and recommendation of technical controls.

- Coordinate information security projects with resources from the IT organization and business unit teams.

- Create and manage a unified and flexible control framework to integrate and normalize the wide variety and ever-changing requirements resulting from global laws, standards and regulations.

- Ensure that security programs are in compliance with relevant laws, regulations and policies to minimize or eliminate risk and audit findings.

- Liaise among the information security team and corporate compliance, audit, legal and HR management teams as required.

- Define and facilitate the information security risk assessment process, including the reporting and oversight of treatment efforts to address findings.

- Manage security incidents and events to protect corporate IT assets, including intellectual property, regulated data and the company's reputation.

- Monitor the external threat environment for emerging threats, and advise relevant stakeholders on the appropriate courses of action.

- Liaise with external agencies, such as law enforcement and other advisory bodies as necessary, to ensure that the organization maintains a strong security posture.

- Develop and oversee effective disaster recovery policies and standards to align with enterprise business continuity management program goals.

- Coordinate the development of incident response plans and procedures to ensure that business-critical services are recovered in the event of a security event.

- Attend professional meetings and seminars as required;

- Provide pro-active performance planning through ePerformance; utilize the ePlan to formalize performance goals, outline professional development plans, and discuss job competencies; utilize the eLogs as an electronic dialogue tool and communication resources for transparent documentation;

- Maintain effective and consistent one on one dialogue with all employees on a regular basis;

- Other duties related to the core functions of this classification.

Minimum Qualifications:

Experience:

Minimum of five years of experience in a combination of risk management, information security and IT jobs. At least two must be in an IT Security leadership role. Three years of professional level experience in computer network and IT systems security associated with a large organization.

Education:

A bachelor degree in Information Security, Computer Science, and Information Management Systems is required or degree related to the core functions of this position. Masters preferred.

Licenses/Certifications:

Professional security management certification, such as a Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA) or other similar credentials, is required.

Examples of Physical and/or Mental Activities:

- Work in a stationary position for long periods of time
- Operates computers, calculators, and other office machines
- May require working extended hours
- May work alone for extended periods of time

Competencies:

http://www.tempe.gov/home/showdocument?id=26274

Job Code: 536

Status: FLSA-Exempt / Classified